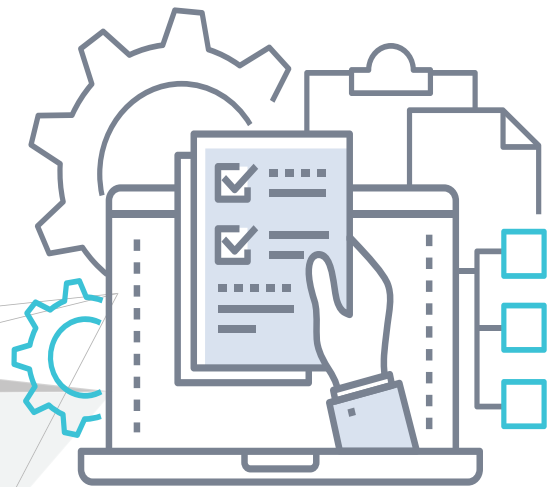


Quick Start Guide for Unitrends MSP Recovery MAX Appliances

Release 10.5.5 | Document Version 1.08102021



Copyright

Copyright © 2021 Unitrends Incorporated. All rights reserved.

Content in this publication is copyright material and may not be copied or duplicated in any form without prior written permission from Unitrends, Inc (“Unitrends”). This information is subject to change without notice and does not represent a commitment on the part of Unitrends.

The software described in this publication is furnished under a license agreement or nondisclosure agreement. The software may be used or copied only in accordance with the terms of the license agreement. See the End User License Agreement before using the software.

The software described contains certain open source components that are copyrighted. For open source licenses, see the Unitrends Open Source Compliance section of the product Administrator Guide.

Because of the nature of this material, numerous hardware and software products are mentioned by name. In most, if not all, cases these product names are claimed as trademarks by the companies that manufacture the products. It is not our intent to claim these names or trademarks as our own.

The following applies to U.S. Government End Users: The Software and Documentation are “Commercial Items,” as that term is defined at 48 C.F.R.2.101, consisting of “Commercial Computer Software” and “Commercial Computer Software Documentation,” as such terms are used in 48 C.F.R.12.212 or 48 C.F.R.227.7202, as applicable. Consistent with 48 C.F.R.12.212 or 48 C.F.R.227.7202 1 through 227.7202 4, as applicable, the Commercial Computer Software and Commercial Computer Software Documentation are being licensed to U.S. Government end users (a) only as Commercial Items and (b) with only those rights as are granted to all other end users pursuant to the terms and conditions herein. Unpublished rights reserved under the copyright laws of the United States. Unitrends agrees to comply with all applicable equal opportunity laws including, if appropriate, the provisions of Executive Order 11246, as amended, Section 402 of the Vietnam Era Veterans Readjustment Assistance Act of 1974 (38 USC 4212), and Section 503 of the Rehabilitation Act of 1973, as amended, and the regulations at 41 CFR Parts 60 1 through 60 60, 60 250, and 60 741. The affirmative action clause and regulations contained in the preceding sentence shall be incorporated by reference.

The following applies to all contracts and subcontracts governed by the Rights in Technical Data and Computer Software Clause of the United States Department of Defense Federal Acquisition Regulations Supplement:

RESTRICTED RIGHTS LEGEND: USE, DUPLICATION OR DISCLOSURE BY THE UNITED STATES GOVERNMENT IS SUBJECT TO RESTRICTIONS AS SET FORTH IN SUBDIVISION (C)(1)(II) OF THE RIGHTS AND TECHNICAL DATA AND COMPUTER SOFTWARE CLAUSE AT DFAR 252 227 7013. UNITRENDS CORPORATION IS THE CONTRACTOR AND IS LOCATED AT 200 WHEELER ROAD, NORTH TOWER, 2ND FLOOR, BURLINGTON, MASSACHUSETTS 01803.

Unitrends, Inc
200 Wheeler Road
North Tower, 2nd Floor
Burlington, MA 01803, USA
Phone: 1.866.359.5411

Contents

Quick Start Guide for Unitrends MSP Recovery MAX Appliances	4
Preparing to configure your Recovery MAX appliance	4
Appliance network requirements	4
Requirements and considerations for DHCP	7
Inspect the appliance	7
Setting up your Recovery MAX appliance	7
Step 1: Set up the appliance on the network	7
Step 2: Set up the appliance using the Quick Setup Wizard	13
Additional details	16

Quick Start Guide for Unitrends MSP Recovery MAX Appliances

The following instructions detail how to configure your Recovery Max appliance, as well as how to prepare it to protect your data.

Preparing to configure your Recovery MAX appliance

First, decide on a location for your appliance. Preferably, a clean, dry area containing power supply and networking capability. For detailed requirements, see the [Site Preparation Guide for Unitrends MSP Recovery MAX appliances](#).

Next, review the "[Appliance network requirements](#)" and determine whether you will configure appliance network settings by using DHCP or manually.

Appliance network requirements

There are several addresses you should permit for all deployments (described in "[Additional ports](#)" below). All of these ports are outgoing connections from the Unitrends appliance. We do not require incoming NAT of ports or exposing the unit to a public IP, only outgoing communication from a local source Unitrends appliance is needed.

IMPORTANT! Never expose the appliance Web UI or SSH connections to open external ports. Doing so may void your support agreement until the appliance can be secured properly. Never deploy the Unitrends appliance on a public IP. All incoming ports to a Unitrends appliance must be firewall protected. Privately operated hot backup copy targets should be deployed in such a way as to secure the VPN connection to only trusted source external IPs

Additional ports

Additional ports must be open if there is a firewall between your appliance and its protected assets, for connectivity to the Internet, and for connectivity to any hot backup copy target. See the following for details:

- "[Connectivity between the appliance and its protected assets](#)"
- "[Connectivity between the appliance and the Internet](#)"
- "[Connectivity between the appliance and a hot backup copy target](#)"

Connectivity between the appliance and its protected assets

Task	Port, Protocol, and Rule	Hostname and IP Address	Notes
Protect assets that are separated from the appliance by a firewall.	<p>1743:</p> <ul style="list-style-type: none"> TCP Outbound from appliance Inbound from protected asset <p>1745:</p> <ul style="list-style-type: none"> TCP Outbound from protected asset Inbound from appliance 	<p>Appliance hostname and IP</p> <p>Asset hostname and IP</p>	<p>If a firewall exists between the appliance and the assets (machines) you wish to protect, open these ports to enable communication and data transfer between the appliance and assets.</p> <p>You must also enter 1745 in the appliance master ini file.</p> <p>To do this:</p> <ol style="list-style-type: none"> In the appliance UI, select Configure > Appliances > Edit > Advanced > General Configuration. In the Configuration Options Section, select data in the Name column. In the Edit Settings dialog, enter 1745 in the Value field and click Save.
Windows assets protected with image-level backups	<p>443:</p> <ul style="list-style-type: none"> TCP Inbound from protected asset 	<p>Appliance hostname and IP</p> <p>Asset hostname and IP</p>	

Connectivity between the appliance and the Internet

Task	Port, Protocol, and Rule	Hostname and IP Address	Notes
Product Updates	<p>20 and 21:</p> <ul style="list-style-type: none"> FTP Outbound <p>80:</p> <ul style="list-style-type: none"> HTTP Outbound 	<p>repo.unitrends.com</p> <p>ftp.unitrends.com</p>	<ul style="list-style-type: none"> repo.unitrends.com is used by the Unitrends appliance to perform software updates. ftp.unitrends.com is used by Support to install patches and updates.

Task	Port, Protocol, and Rule	Hostname and IP Address	Notes
Remote Support	443: <ul style="list-style-type: none"> • HTTPS • Outbound 	support-itivity.unitrends.com 74.202.224.68	Used for opening a remote tunnel to the Unitrends support team.
Proactive Monitoring	161 and 162: <ul style="list-style-type: none"> • TCP and UDP • Outbound 	notifications.unitrends.com 104.130.228.89	Used for SNMP trap collection for all proactive monitoring.

Connectivity between the appliance and a hot backup copy target

Task	Port, Protocol, and Rule	Hostname and IP Address	Notes
Backup copy to the Unitrends Cloud or your Unitrends target appliance.	The OpenVPN port provided by Unitrends Or The port number you have configured for the secure tunnel connection to the backup copy target appliance. <ul style="list-style-type: none"> • TCP and UDP • Outbound 443: <ul style="list-style-type: none"> • TCP • Outbound 	Target appliance hostname and IP For Unitrends Cloud, the public-facing IP address provided by Unitrends.	Used for copying data to the Unitrends Cloud or your Unitrends target appliance.

If DHCP is available in your environment, review the ["Requirements and considerations for DHCP"](#) before proceeding.

If DHCP is not available in your environment, or if you intend to use this appliance as a backup copy target, the following information is required for network configuration:

- An IP address to assign to the appliance.
- The netmask value for your organization.
- A gateway IP address.
- An IP address for networked DNS servers.
- A network domain name.

Note: You can obtain the above information from your network administrator.

Requirements and considerations for DHCP

- If your environment goes offline for an extended period of time, your appliance may be assigned a new IP address from the DHCP server. This may cause a temporary loss of backup and recovery functionality. If this occurs, see [KB 360013261398](#) for instructions on how to proceed.
- The eno1 adapter is, by default, configured for DHCP.
- DHCP cannot be configured for more than one network adapter at any given time.
- A network adapter configured for DHCP cannot be managed via the appliance user interface (UI) described in the [Administrator Guide for Recovery Series, Recovery MAX, and Unitrends Backup](#) unless you intend to assign it a static IP address.
- Unitrends appliances intended for use as backup copy targets must be assigned static IP addresses.

Inspect the appliance

After unpacking the appliance, check for physical damage that may have occurred during shipping. To report shipping damage or missing items, please contact support at support@unitrendsmsp.com or 1-866-881-4766.

Setting up your Recovery MAX appliance

There are two basic steps to setting up your appliance:

- ["Step 1: Set up the appliance on the network"](#).
- ["Step 2: Set up the appliance using the Quick Setup Wizard" on page 13](#)

Step 1: Set up the appliance on the network

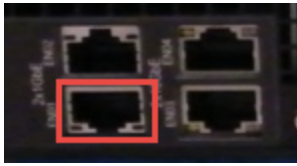
Your appliance ships with the required software already installed. In addition, the appliance is already registered with the correct license. You do not need to install anything on the appliance. To get started, simply power on the appliance and configure its network settings right from the console. Once you have configured network settings, you can perform all administration tasks from any workstation by connecting to the appliance User Interface (UI). Depending on the capabilities of your environment, choose one of the following procedures:

- ["To set up the appliance with DHCP "](#)
- ["To set up the appliance with a static IP address " on page 9](#)

To set up the appliance with DHCP

CAUTION! Ensure that you reviewed the ["Requirements and considerations for DHCP" on page 7](#) before proceeding.

- 1 Attach a monitor, keyboard, and mouse to the appliance.
- 2 Connect your network cable to the eno1 adapter located on the front of the appliance:



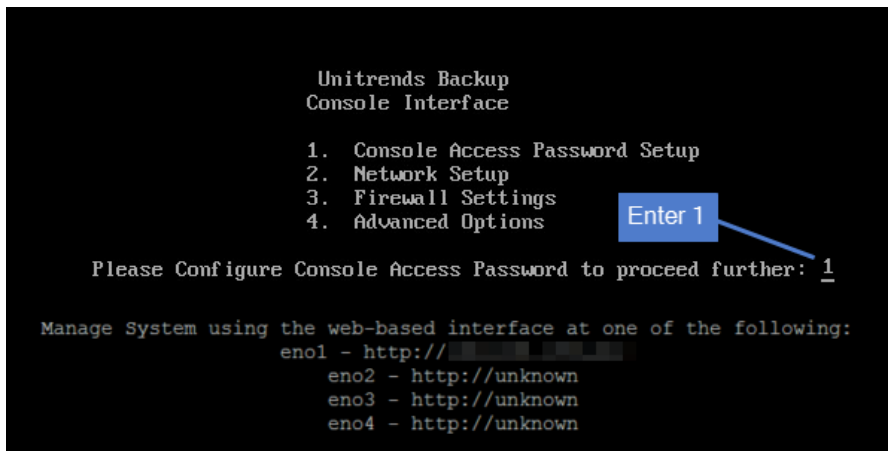
3 Power on the appliance.

- DHCP automatically assigns an IP address to the appliance when you power it on for the first time.
- When the appliance is powered on, you see a list of menu choices in the Unitrends Backup Console Interface.

Notes:

- As you complete each step in the Unitrends Backup Console Interface, you are presented with the next configuration screen.
- You can press **Enter** to accept the default or current setting.

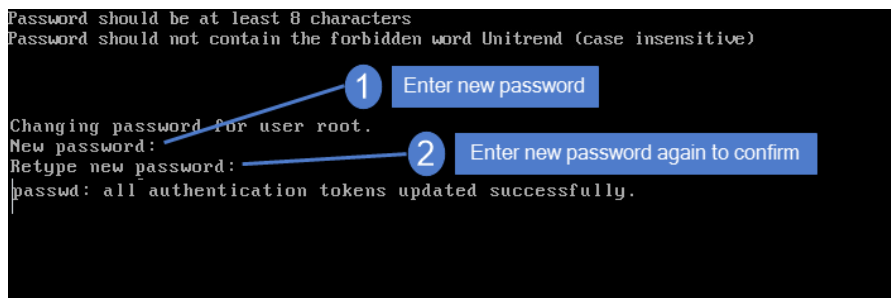
4 On the Console Interface screen, enter **1** in the **Please Configure Console Access Password...** field.



5 To change the direct console password, enter a new password, then enter the password again to confirm.

Notes:

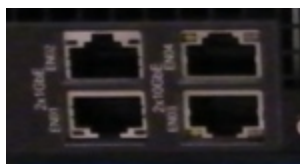
- This is the root operating system password that accesses the console. This password does not access the UI. (You will change the UI password in "[Step 2: Set up the appliance using the Quick Setup Wizard](#)" on page 13.)
- All appliances are deployed with these default operating systems credentials: user *root*, password *unitrends1*. For appliance security, you must change this password.



You can complete the setup remotely from any workstation or server on the network by accessing the appliance at <https://<appliance IP address>>. You can find the IP address at the bottom of the Unitrends Backup Console Interface screen. Proceed to "[Step 2: Set up the appliance using the Quick Setup Wizard](#)".

To set up the appliance with a static IP address

- 1 Attach a monitor, keyboard, and mouse to the appliance.
- 2 Connect your network cable to one of the four ports located on the front of the appliance and note your chosen adapter. (See the image below.)



- 3 Power on the appliance.

When the appliance is powered on, you see a list of menu choices in the Unitrends Backup Console Interface.

Notes:

- As you complete each step in the Unitrends Backup Console Interface, you are presented with the next configuration screen.
- You can press **Enter** to accept the default or current setting.

- 4 On the Console Interface screen, enter **1** in the **Please Configure Console Access Password...** field.

```

Unitrends Backup
Console Interface

1. Console Access Password Setup
2. Network Setup
3. Firewall Settings
4. Advanced Options
Enter 1

Please Configure Console Access Password to proceed further: 1

Manage System using the web-based interface at one of the following:
eno1 - http://
eno2 - http://unknown
eno3 - http://unknown
eno4 - http://unknown

```

- 5 To change the direct console password, enter a new password, then enter the password again to confirm.

Notes:

- This is the root operating system password that accesses the console. This password does not access the UI. (You will change the UI password in "Step 2: Set up the appliance using the Quick Setup Wizard" on page 13.)
- All appliances are deployed with these default operating systems credentials: user *root*, password *unitrends1*. For appliance security, you must change this password.

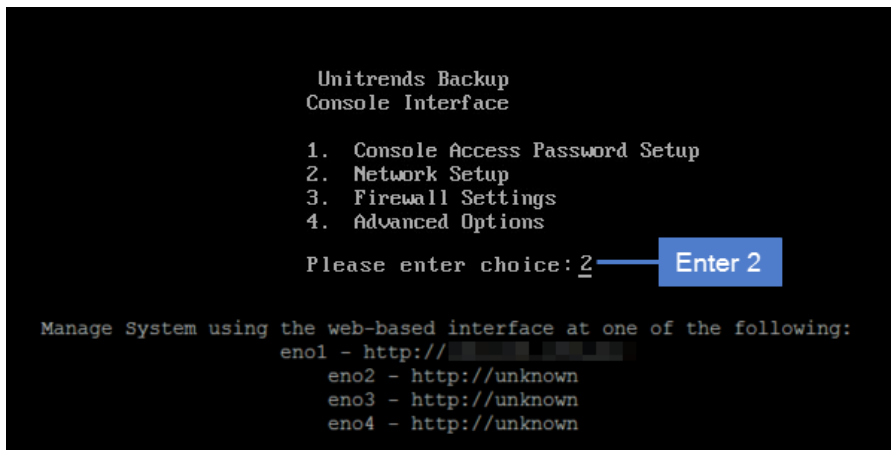
```

Password should be at least 8 characters
Password should not contain the forbidden word Unitrend (case insensitive)

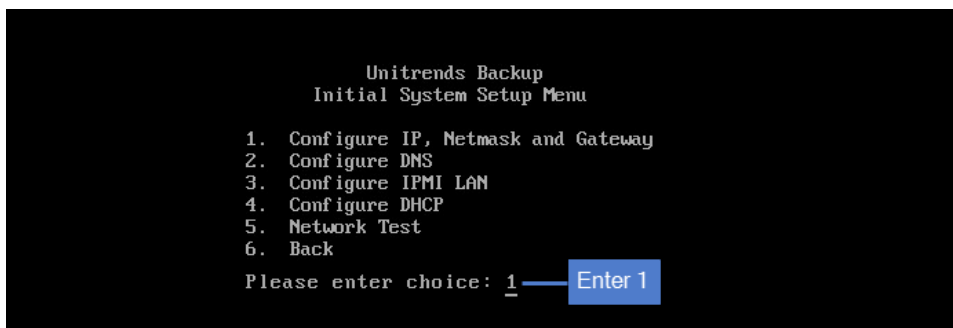
Changing password for user root.
New password:
Retype new password:
passwd: all authentication tokens updated successfully.

```

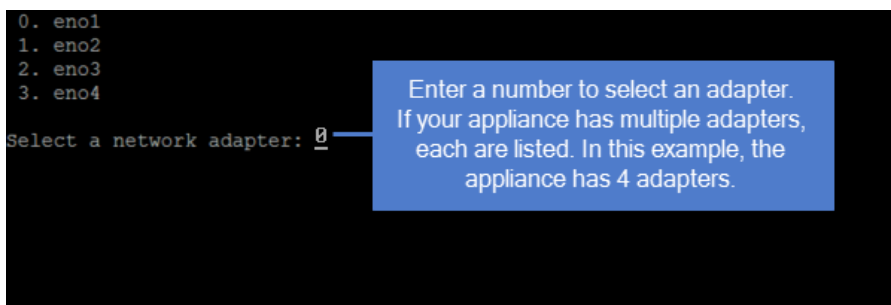
- 6 On the Console Interface screen, enter 2 in the **Please enter choice** field.



7 On the Initial System Setup Menu screen, enter **1** in the **Please enter choice** field.



8 Enter a number in the **Select a network adapter** field. For example, enter **0** to select eno1.



Note: On some appliances, the first Ethernet port (eno1) is also configured for IPMI with DHCP. You can use IPMI for advanced troubleshooting. The default IPMI credentials are user ADMIN and password ADMIN. Change this password for security reasons. See the [KB 360013151657](#) for details.

9 Enter **Y** to configure the IP address, netmask, and gateway. Follow the prompts to enter each setting. Review your settings, then enter **Y** to commit the network configuration changes.

```

Network Adapter:   en01
Current IP address: 10.10.10.1
Current Netmask:   "255.255.255.0"
Current Gateway:   n/a

Edit network configuration? [n/Y]: Y

```

Enter Y

```

Current IP address: 10.10.10.1
Enter new System IP Address: 192.168.1.20

```

Enter an IP address for the Unitrends appliance

```

Current Netmask: "255.255.255.0"
Enter new System Netmask:

```

Enter new netmask or press Enter to accept the default

```

Current Gateway: n/a
Enter new Network Gateway: 192.168.1.1

```

Enter gateway IP address

```

Adapter:           en01
Current IP address: 10.10.10.1
Current Netmask:   "255.255.255.0"
Current Gateway:   n/a

New IP address:     192.168.1.20
New Netmask:        "255.255.255.0"
New Gateway:        192.168.1.1

Commit network configuration changes? [n/Y]: Y

```

Enter Y to save settings (or N to modify settings)

- 10 To configure DNS settings, enter **2**, then enter **Y** to edit. Enter the **Primary DNS IP address**, a **Secondary DNS IP** (optional), and a **DNS Domain**. Review the settings and enter **Y** to save.

```

Unitrends Backup
Initial System Setup Menu

1. Configure IP, Netmask and Gateway
2. Configure DNS
3. Configure IPMI LAN
4. Configure DHCP
5. Network Test
6. Back

Please enter choice: 2

```

Enter 2

```
Current Primary DNS: n/a
Current Secondary DNS: n/a
Current DNS Domain: 
Edit DNS configuration? [n/Y]: Y
```

Enter Y

```
Current Primary DNS: n/a
Enter new Primary DNS: 192.168.1.108
```

Enter IP of primary DNS server

```
Current Secondary DNS: n/a
Enter new Secondary DNS: 192.168.1.108
(Leave blank if no secondary DNS desired)
```

(Optional) Enter IP of secondary DNS server

```
Current DNS Domain: 
Enter new DNS Search Domain: unitrends.com
```

Enter domain

```
Current Primary DNS: n/a
Current Secondary DNS: n/a
Current DNS Domain: 
New Primary DNS: 192.168.1.108
New Secondary DNS: 192.168.1.108
New DNS Domain: unitrends.com
Commit DNS configuration changes? [n/Y]: Y
```

Enter Y to save settings (or N to modify settings)

11 To exit network setup, enter 6.

```
Unitrends Backup
Initial System Setup Menu

1. Configure IP, Netmask and Gateway
2. Configure DNS
3. Configure IPMI LAN
4. Configure DHCP
5. Network Test
6. Back

Please enter choice: 6
```

Enter 6

You have finished configuring network settings. You can complete the setup remotely from any workstation or server on the network by accessing the appliance at <https://<appliance IP address>>. You can find the IP address at the bottom of the Unitrends Backup Console Interface screen. Proceed to "Step 2: Set up the appliance using the Quick Setup Wizard".

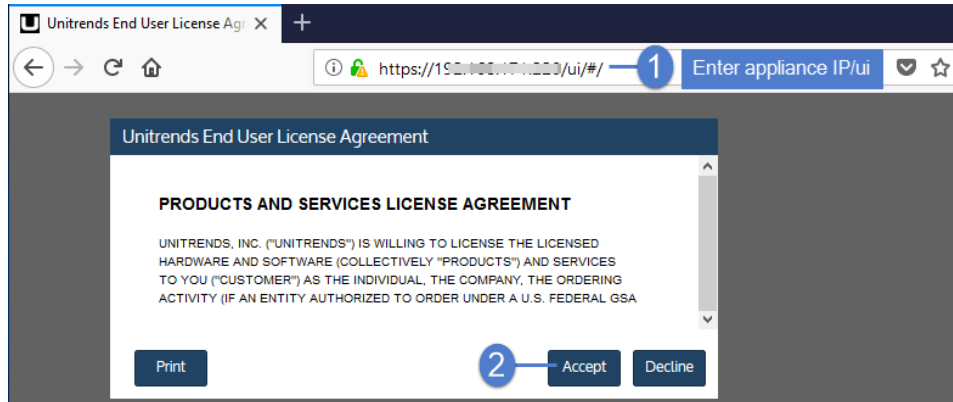
Step 2: Set up the appliance using the Quick Setup Wizard

To start the setup process, you will log in to the appliance UI from any machine on the same network by opening a browser and entering the appliance's IP address followed by `/ui/`. The Quick Setup Wizard launches when you access

the UI for the first time.

To set up the appliance

- 1 Open a browser and connect to your appliance by entering: **https://<applianceIP>/ui**. For example: **https://10.10.10.1/ui**.
- 2 Click **Accept** to accept the license agreement.



- 3 Set the appliance date and time by doing one of the following, then click **Next**:


- Select a **Timezone**. If needed, modify the appliance **Date** and **Time**.

OR

- Check the **Use an NTP Server** box to sync to an NTP server. (Optional) Enter your preferred NTP server address.


UNITRENDS

Date & Time
Host Name & Password
Email



Crazy-committed to helping you play IT safe.


Enter a date and time for your appliance

Date 

Time

Time Zone

Use an NTP Server

NTP Server Addresses 

0.centos.pool.ntp.org

1.centos.pool.ntp.org

Click to continue
Next

- 4 Enter a **Host Name**, a **Domain**, and a new **UI Password** for the appliance. Confirm the UI password by entering it again in the field to the right. Click **Next**.

Notes:

- The hostname can contain only alphanumeric characters, dashes, and underscores.
- The appliance has a UI root user and an OS root user. These are separate accounts. Changing the password of one root user account does NOT change the password of the other root user account. The UI root user is used to log in to the appliance UI. The OS root user is used to log in to the appliance console or for command line access.
- Because you have already set the OS password, these fields are disabled in the Quick Setup Wizard.
- Passwords cannot contain the word *Unitrend* (case insensitive).
- All appliances are deployed with these default UI credentials: user *root*, password *unitrends1*. For appliance security, you must change this password in the Quick Setup Wizard. For increased security, ensure that the OS password you enter is different than the UI user password you entered in [Step 1](#).
- After you finish the deployment procedures in this guide, you can set up additional UI users for the appliance at any time. For details, see *Users and roles* in the [Administrator Guide for Recovery Series, Recovery MAX, and Unitrends Backup, Appliance settings](#) topic.

- 5 (Optional) To enable email from the appliance, check **Enable email reporting** and enter the following:
 - The fully qualified domain name of the **SMTP server**.
 - (If needed) If the SMTP server requires authentication, select **Authentication required** and enter a **Username** and **Password**.
 - Click **+ Add Recipients** to add an email recipient. Enter an email address in the **Recipient** field and select one or more of the **System**, **Jobs**, and **Failures** options to specify which reports the appliance will send to the recipient. Repeat as needed to add more recipients.

6 Click **Finish**.

UNITRENDS

Date & Time | Host Name & Password | **Email**

1 Enable email reporting

SMTP Server: unitrends.com

Authentication Required

2 Enter the FQDN of the SMTP server

3 If the SMTP server uses authentication, check the box and enter credentials

4 + Add Recipients
Click to add an email recipient

Recipients	System	Jobs	Failures
jalvarez@unitrends.com	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
djones@unitrends.com	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

5 For each recipient, enter an email address and select reports to send

6 Previous Finish

When the dialog completes, a short tour begins to help you get started.

Additional details

Reference the [Administrator Guide for Recovery Series, Recovery MAX, and Unitrends Backup](#) on the Unitrends website.

IMPORTANT! Record the appliance asset tag, which is a 10-11 digit string on the appliance. To see the string, select ? > **About** in the UI. When you contact support, you may need this information.

Appliance Asset Tag: _____